Amendments to the Specification:

Please replace the abstract of the invention with the following new abstract:

--A method and devices for a control of usage of content is disclosed. In one embodiment, a user device performs the steps of obtaining the content, defining usage rights, generating integrity protection information for defined usage rights, encrypting the content with a content encryption key, encrypting the content encryption key with a key encryption key associated with a recipient device and/or an operator of the recipient device, communicating the encrypted content, the defined usage rights, the encrypted content encryption key, and the integrity protection information to the recipient device. The recipient device performs the steps of verifying the integrity of the defined usage rights based on the integrity protection information, decrypting the encrypted content encryption key with a decryption key corresponding to the key encryption key, decrypting the encrypted content with the content encryption key in a secure environment, applying the defined usage rights to the content in the secure environment, and using the content according to the applied usage rights.--

Please amend paragraph [0064] as follows:

-- [0064] Typically, definition and processing of usage rights is defined in a positive manner only those usage rights that are defined and communicated to the recipient device D2 can be applied for the usage of the content at the recipient device D2, i.e. if no usage rights are defined and communicated, e.g. for an empty rights object, no rights are assigned to the recipient device D2 and usage of the content is not allowed at all. Depending on the implementation of the invention, usage rights may be defined and processed the opposite way, i.e. to allow all kind of usages if no usage rights are defined and communicated and to define only those usage rights for which no usage at the recipient device D2 is allowed. Thus, implementation of the invention is preferably according to a standardized or ~~de-fact~~ de-facto standardized solution and a verification to which kind of standard at least the recipient device D2 complies may be performed

before communicating the usage rights to or applying the usage rights at the recipient device D2 in order to ensure that the content is used according to the defined usage rights. Thus, an implementation based on compliant user and recipient devices can be of advantage. –

Please amend paragraph [0065] as follows:

-- [0065] Combinations of usage rights are possible, i.e. a usage right can comprise one or more of the usage rights in the form of usage restrictions and/or usage permissions, e.g. those listed above. Alternatively, or in addition, usage rights can be defined and communicated separately, e.g. each usage right comprising only one usage restriction or usage permission. An example for a combination of usage rights is to allow a 1-month usage with unlimited number of usages without permitting a forwarding or duplication. –

Please amend paragraph [0085] as follows:

-- [0085] The rights server DS can respond after verifying contents of the message X110 by message X120 denoted by DS Hello. Message ~~120~~ X120 can comprise an identity identifying the rights server DS towards the recipient device D2 as well as supported version numbers, supported security algorithms, a rights issuer nonce, status information, and a session identity as well as further information like the list of trusted authorities or extensions. Although described as single messages, messages X110, X120 can consist also of several messages. –

Please amend paragraph [0131] as follows:

-- [0131] Referring now to FIG. 5b, which depicts an embodiment for a recipient device D2. Corresponding to the user device D1, the recipient device D2 comprises a receiving unit RU2 and a transmission unit TU2 for receiving and sending, respectively, of messages according to the invention. Furthermore, the recipient device D2 comprises a

processing unit PU2 and a secure environment SE2 for processing and using encrypted content according to the defined usage rights. The content can be used according to the defined usage rights e.g. by the processing unit PU2 itself, at an output unit OU2, or for forwarding via a transmission unit TU2. Furthermore, the processing unit PU2 can be adapted to define further usage rights being a subset of the usage rights for the content in the secure environment, e.g. based on an instruction entered via input unit IU2, and to send the further usage rights to the user device D1 via the transmission unit TU2. The processing unit PU2 can be adapted to interface with a storage unit DB2 and to perform further steps and processes of the invention as far as related to the recipient device D2. --